

CLAIMS

What is Claimed is:

1. A method of managing utilization of network intrusion detection systems in a dynamic data center, said method comprising:
 - 5 providing a plurality of network intrusion detection systems, each being networked so that utilization of each network intrusion detection system can be based on demand for said network intrusion detection systems in said dynamic data center;
 - receiving a monitoring policy and a plurality of monitoring points to be
10 monitored on a network with any of said network intrusion detection systems; and
 - automatically arranging the monitoring of said monitoring points using said network intrusion detection systems and said monitoring policy.
- 15 2. The method as recited in Claim 1 wherein said automatically arranging the monitoring of said monitoring points includes:
 - automatically configuring a plurality of network resources to provide network communication data from said monitoring points to a plurality of available network intrusion detection systems from said network intrusion
20 detection systems; and
 - automatically configuring said available network intrusion detection systems to receive said network communication data based on said monitoring policy.
- 25 3. The method as recited in Claim 2 wherein said automatically arranging the monitoring of said monitoring points further includes:
 - automatically increasing a number of particular network intrusion detection systems receiving said network communication data from a particular monitoring point by selecting additional available network
30 intrusion detection systems if said network communication data exceeds a capacity of said particular network intrusion detection systems.

4. The method as recited in Claim 2 wherein said automatically arranging the monitoring of said monitoring points further includes:

5 automatically decreasing a number of particular network intrusion detection systems receiving said network communication data from a particular monitoring point by releasing any of said particular network intrusion detection systems to said available network intrusion detection systems if said network communication data is below a predetermined threshold of a capacity of said particular network intrusion detection systems.

10

5. The method as recited in Claim 2 wherein said network resources include one of a firewall, a gateway system, a network switch, and a network router.

15 6. The method as recited in Claim 1 wherein said receiving a monitoring policy and a plurality of monitoring points to be monitored includes:

providing a graphical user interface to receive said monitoring policy and said plurality of monitoring points to be monitored.

20

7. The method as recited in Claim 1 wherein said dynamic data center is a utility data center.

25 8. A computer-readable medium comprising computer-executable instructions stored therein for performing a method of managing utilization of network intrusion detection systems in a dynamic data center, said method comprising:

30 providing a plurality of network intrusion detection systems, each being networked so that utilization of each network intrusion detection system can be based on demand for said network intrusion detection systems in said dynamic data center;

receiving a monitoring policy and a plurality of monitoring points to be monitored on a network with any of said network intrusion detection systems; and

5 automatically arranging the monitoring of said monitoring points using said network intrusion detection systems and said monitoring policy.

9. The computer-readable medium as recited in Claim 8 wherein said automatically arranging the monitoring of said monitoring points includes:

10 automatically configuring a plurality of network resources to provide network communication data from said monitoring points to a plurality of available network intrusion detection systems from said network intrusion detection systems; and

15 automatically configuring said available network intrusion detection systems to receive said network communication data based on said monitoring policy.

20 10. The computer-readable medium as recited in Claim 9 wherein said automatically arranging the monitoring of said monitoring points further includes:

25 automatically increasing a number of particular network intrusion detection systems receiving said network communication data from a particular monitoring point by selecting additional available network intrusion detection systems if said network communication data exceeds a capacity of said particular network intrusion detection systems.

11. The computer-readable medium as recited in Claim 9 wherein said automatically arranging the monitoring of said monitoring points further includes:

30 automatically decreasing a number of particular network intrusion detection systems receiving said network communication data from a

particular monitoring point by releasing any of said particular network intrusion detection systems to said available network intrusion detection systems if said network communication data is below a predetermined threshold of a capacity of said particular network intrusion detection systems.

5

12. The computer-readable medium as recited in Claim 9 wherein said network resources include one of a firewall, a gateway system, a network switch, and a network router.

10

13. The computer-readable medium as recited in Claim 8 wherein said receiving a monitoring policy and a plurality of monitoring points to be monitored includes:

providing a graphical user interface to receive said monitoring policy and said plurality of monitoring points to be monitored.

15

14. The computer-readable medium as recited in Claim 8 wherein said dynamic data center is a utility data center.

15. A system comprising:

20 a dynamic data center including:

a plurality of network resources;

a plurality of network intrusion detection systems, each being networked so that utilization of each network intrusion detection system can be based on demand for said network intrusion detection systems in said

25 dynamic data center;

a graphical user interface for receiving a monitoring policy and a plurality of monitoring points to be monitored on a network with any of said network intrusion detection systems; and

30 a controller for controlling said network resources and said network intrusion detection systems and for automatically arranging the

monitoring of said monitoring points using said network intrusion detection systems and said monitoring policy.

16. The system as recited in Claim 15 wherein said controller
5 automatically configures said network resources to provide network
communication data from said monitoring points to a plurality of available
network intrusion detection systems from said network intrusion detection
systems, and wherein said controller automatically configures said available
network intrusion detection systems to receive said network communication
10 data based on said monitoring policy.

17. The system as recited in Claim 16 wherein said controller
automatically increases a number of particular network intrusion detection
systems receiving said network communication data from a particular
15 monitoring point by selecting additional available network intrusion
detection systems if said network communication data exceeds a capacity of
said particular network intrusion detection systems.

18. The system as recited in Claim 16 wherein said controller
20 automatically decreases a number of particular network intrusion detection
systems receiving said network communication data from a particular
monitoring point by releasing any of said particular network intrusion
detection systems to said available network intrusion detection systems if
said network communication data is below a predetermined threshold of a
25 capacity of said particular network intrusion detection systems.

19. The system as recited in Claim 15 wherein said network
resources include one of a firewall, a gateway system, a network switch, and
a network router.

30

200209600-1

20. The system as recited in Claim 15 wherein said dynamic data center is a utility data center.